National Infrastructure Protection Center
NIPC Daily Open Source Report
for 09 January 2003

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
www.whitehouse.gov/homeland

Daily Overview

- A new initiative is forming to focus on cyber security in the chemical industry, under the auspices of the Chemical Industry Data Exchange (CIDX) trade association. On Tuesday the CIDX and the Chemicals Sector Cyber−Security Information Sharing Forum announced the launch of the Chemicals Sector Cyber−Security Practices, Standards and Technology Initiative. (See item 3)

- Global Security Newswire reports the Defense Department has a research program to develop new sensors to identify, in less than 60 seconds, biological warfare agents dispersed in aerosol form. (See item 11)

- CERT has released Vulnerability Note VU#412115: "Network device drivers reuse old frame buffer data to pad packets." (See item 18)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 08, Associated Press* — **Safety concerns nuclear agency workers.** The top officials of the Nuclear Regulatory Commission say it is committed to safety, but they're having trouble convincing many of the agency's own workers. **A survey of NRC employees shows that a third of them question the agency's commitment to public safety and nearly half are not comfortable raising concerns about safety issues within the agency.** The survey, conducted by a private consulting firm, found the NRC's overall "safety culture and climate" has improved since a similar 1998 survey. It also emphasizes that the findings demonstrated that NRC

employees are committed to protecting public safety at the nation's nuclear power plants. But the survey – which covered about half of the agency's 3,072 employees, from clerical workers to nuclear engineers to senior managers – also showed that nearly half of them don't feel that it's "safe to speak up in the NRC" about safety issues. And a majority of the workers complained the agency "has not established a climate where traditional ways of doing things can be challenged," according to the 41−page report released by the NRC's inspector general and posted on the agency Web site. **When asked a series of questions assessing agency attitudes toward safety and employee involvement in how the agency addresses safety issues, 67 percent of the workers responded favorably and 33 percent unfavorably.** The "2002 Survey of NRC's Safety Culture and Climate" was conducted by International Survey Research LLC, a private firm hired by the NRC.
Source: http://www.washingtonpost.com/wp−dyn/articles/A25981−2003Jan8.htm l

2. *January 07, Associated Press* — **Company seeks OK to power up cable. The Cross Sound Cable Co. is making another bid to power up its 24−mile−long electric cable across Long Island Sound.** The cable was laid last spring, but regulators have refused to allow its use **because it was not sunk deep enough in parts of New Haven Harbor to meet conditions of the approval.** The company has now asked the Connecticut Siting Council to clarify its approval and allow use of the cable while the company works “in good faith" to resolve the problems. **“Based on the fact that it is safely buried, and it has no environmental impacts, we feel we should be able to operate while we continue to work toward the authorized depths,"** Cross Sound spokeswoman Rita Bowlby said Monday. Cross Sound Cable maintains that the state environmental agency and the U.S. Army Corps of Engineers agree the cable would pose no environmental or safety problems were it to be energized today. The request will be considered by the Siting Council on Wednesday and faces opposition from the state Department of Environmental Protection and Attorney General Richard Blumenthal. The state went to court last summer when the company threatened to unilaterally energize the cable. **The state forced the company to stipulate before a judge that it would not energize the line until it met all conditions of its permit approvals.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=ap_2003_01_07_−−−−−_5158−4636−CT−−CrossSoundCable.1stLd−Writethru.a>

[Return to top]

Chemical Sector

3. *January 08, eSecurity Planet* — **Chemical industry seeks formula for cyber security.** A new initiative is forming to focus on cyber security in the chemical industry, under the auspices of the Chemical Industry Data Exchange (CIDX) trade association. **On Tuesday the CIDX and the Chemicals Sector Cyber−Security Information Sharing Forum announced the launch of the Chemicals Sector Cyber−Security Practices, Standards and Technology Initiative.** The Initiative, to be implemented by a new CIDX business unit, will be **charged with finding ways to improve the base level of security in the chemical industry.** The Chemicals Sector Cyber−Security Information Sharing Forum was formed in early 2002 and consists of senior−level executives representing 10 chemical industry trade asociations and more than 2,000 companies. **The group has already identified existing cyber security practices and**

standards, and hopes to build on them to reach concensus for a set of security standards specific to the chemical industry.
Source: http://www.esecurityplanet.com/trends/article/0,,10751_1566371,00 .html

[Return to top]

Defense Industrial Base Sector

4. *January 08, Associated Press* — **Pentagon cancels two missile intercept tests, saving $200 million.** The Pentagon agency that is developing defenses against missile attack has decided to skip two tests of its ability to intercept mock warheads in space, saving about $200 million, an official said Wednesday. The tests were to have been held this winter and spring. **Air Force Lt. Col. Rick Lehner, spokesman for the Missile Defense Agency, said there will not be another intercept test until Boeing Co., the lead contractor, has a newly designed rocket booster ready for use this autumn. "The feeling is that we need to concentrate on the booster this year because it is behind" schedule, Lehner said.** Boeing originally was to begin flight tests of a new booster — used to carry a missile−intercept device known as a "kill vehicle" into space to destroy an enemy warhead by colliding with it — in 2000, but it encountered technical problems. After a booster launch failure in December 2001, Boeing decided to contract with Lockheed Martin, and later Orbital Sciences, to come up with new designs for an intercept booster.
Source: http://story.news.yahoo.com/news?tmpl=storyp_wo_en_po/na_gen_us_missile_defense_1

[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

5. *January 08, Washington Post* — **21 killed in plane crash at North Carolina airport. A US Airways Express commuter plane carrying 19 passengers and two crew members smashed into a maintenance hangar and exploded while taking off from the Charlotte−Douglas International Airport shortly before 9 a.m. Wednesday morning.** All on board Flight 5481 were killed, authorities and airline officials said. The plane, which had been scheduled to take off at about 8:30 a.m. for an hour−long flight to the Greenville−Spartanburg International Airport in South Carolina. Witnesses at the airport reported seeing a fireball and smoke after the accident. "The plane is so destroyed there's not much to see," Charlotte police spokesman Keith Bridges told the Associated Press. "The debris is in such bad shape." **An FBI official in Charlotte told reporters there was no indication of terrorism.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A26675−2003Jan8.htm l

6. *January 08, Atlanta Journal−Constitution* — **Blast−proof cargo bin in development.** Rick Fingerhut, a recognized expert on plane explosions, and a team of engineers have spent the past 10 years **developing a blast−proof cargo container they hope will put an end to such terrorist bombings. The Transportation Security Administration purchased five of the containers last fall to test in flight. The flexible sides of the container, designed to bulge but not break in a blast, are made of a composite variant of Kevlar, which is widely used in bulletproof vests.** But the container's weight could be an obstacle. The blast−proof containers weigh 343 pounds, compared with 187 pounds for a regular container. Heavier aircraft use more fuel, one of the biggest expenses for airlines. A spokesman for the company developing that container says that they have also developed an ultra−light cargo container that weighs only 143 pounds. If an airline used a handful of blast−proof containers on each flight for suspect bags and put the rest in ultra−light containers, the weight issue would be a wash, the spokesman said.
   Source: http://www.accessatlanta.com/ajc/business/delta/0103/08cargo.html

7. *January 08, Associated Press* — **Man faces trespass charge for allegedly sneaking onto jet.** A man bypassed airport security and gained access to an empty jetliner, later telling deputies he "wanted to take a plane ride," authorities said. **Richard N. Moore, 40, allegedly sneaked into the ramp area of Florida's St. Petersburg−Clearwater International Airport on Tuesday and climbed a stairway into the American Trans Air 737.** Miguel Santos, an ATA mechanic who was working on the wing of another aircraft, told authorities he saw Moore get in the plane, then followed him inside, where he found him sitting in a seat in the 10th row. Santos then called police. "Obviously, it's some kind of breach, and we're going to check that out," said Brian Doyle, a spokesman for the Transportation Security Administration, the federal agency that oversees security at 429 airports nationwide. Investigators checked the plane and surrounding area with bomb−sniffing dogs but found no explosives.
   Source: http://www.cnn.com/2003/TRAVEL/01/08/airport.trespassing.ap/

[Return to top]

Postal and Shipping Sector

8. *January 09, Business Times* — **West Coast dockers vote on contract. US West Coast dockworkers began voting on a tentative contract deal reached after a bitter labor dispute that led to a 10−day shutdown of ports handling $300 billion of cargo each year.** A caucus of the International Longshore &Warehouse Union in December recommended that the 10,500 rank and file members approve the six−year deal that boosts wages and benefits but will lead to some job losses due to new technology. The union will announce the result of the vote on Jan 22, said ILWU spokesman Steve Stallone. **If approved, the tentative deal brokered by a federal mediator takes immediate effect.**
   Source: http://business−times.asia1.com.sg/shippingtimes/story/0,2276,689 89,00.html?

9. *January 04, Ottawa Citizen* — **Port security is Canada's 'weakest link'.** Canada's inability to detect a terrorist nuclear weapon hidden on a cargo ship is one of the weakest links in the country's security, warns a government panel of scientists and industry officials. **Slipping a nuclear weapon or radiological "dirty bomb" into a sea container on a freighter is the likeliest way terrorists would try to get such devices into North America, says a May 2002**

report prepared by the Defence Science Advisory Board. Such a scenario involving the delivery of the **weapon "directly to port, but intended for use prior to any inspection is perhaps the highest probability,"** concludes the study, obtained by the Citizen under the Access to Information law. "This makes ports the highest probability targets in North America for certain types of (weapons of mass destruction) should they be acquired by terrorists." **Current technology cannot detect nuclear bombs if they are hidden in sea containers and the board recommends the government conduct an aggressive research program into developing new sensor systems to ferret out such weapons.** "This lapse in maritime security may be our weakest link," it warns.
Source: http://canada.com/national/story.asp?id={E9BCCD31−BE8A−407E−904C−5F963B0E9843}

[Return to top]

Agriculture Sector

10. *January 08, AgWeb* — **State of emergency declared for California's Newcastle Disease. California governor Gray Davis today declared a state of emergency in the fight against an outbreak of Exotic Newcastle Disease among poultry in Southern California.** The emergency declaration will enable state agencies to pool resources and work cooperatively with the California Department of Food and Agriculture in addressing the response to the incident. Emergency declarations are the customary means for the state to streamline such responses.
Source: http://www.agweb.com/news_show_news_article.asp?file=AgNewsArticle_2003181541_5012newscat=GN

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

11. *January 08, Global Security Newswire* — **Pentagon seeks improved sensors for aerosol attacks. The Defense Department last week launched a crash research program to develop new sensors to rapidly identify, in less than 60 seconds, biological agents dispersed in aerosol form, according to a Defense Advanced Research Projects Agency (DARPA) announcement.** The effort will focus on technologies that can detect optical characteristics, invisible to the naked eye, of biological agents released in vapor or spray form, according to a

project description. DARPA said it is seeking proposals to design and develop "high−risk, high−leverage technologies and prototypes that have the potential to greatly reduce the false alarm rate of trigger sensors for biological warfare agents." **The effort, which is seeking proposals from qualified corporations, research centers, and universities, would support a Pentagon−wide program to develop the first multilayered, nationwide biological detection system to defend highly populated areas from germ warfare.**
Source: http://www.govexec.com/dailyfed/0103/010803gsn1.htm

12. *January 05, Alameda Times−Star* — **Shortage of beds and nurses threatens stressed system. Timely emergency care for seriously ill or injured patients is a service that hospitals nationwide now struggle to provide.** And hospital officials are convinced that, without fundamental changes, the situation will only worsen as more people flock to a shrinking number of ERs for care they can't get elsewhere. ``We are the place of first and last resort with a health care system that seems truly broken," said Dr. Mary Rutherford, the director of emergency medicine at Children's Hospital Oakland. ``The ER seems to be a giant Band Aid that keeps it all together." Michael Mahoney, CEO of St. Rose Hospital in Hayward, said he's ``worried every day," about the future of hospitals in Alameda, California. He said the emergency care system is on the brink. **An array of forces converges to create the perilous ER situation. A shortage of hospital beds and nursing staff, ER closures, sicker patients, a lack of access to regular doctors by both the uninsured and the insured, and unpaid ER bills are all creating what Bay Area emergency care workers interviewed for this story unanimously called a crisis.** Essentially, the crisis facing ERs boils down to finances: ERs are often money−losing propositions for hospitals and doctors. In 2000, 80 percent of California's emergency departments operated in the red, losing $425 million in hospital charges and unreimbursed doctors' fees, according to the California Medical Association. So hospitals close them, or consolidate ERs as hospitals are purchased and merged.
Source: http://www.timesstar.com/cda/article/print/0,1674,125%257E10859%257E1091117,00.html

[Return to top]

Government Sector

13. *January 08, Associated Press* — **Veteran law enforcement official to head Secret Service.** A law enforcement official with a 28−year career at the Secret Service was tapped Wednesday to be director of the agency. **For the past year, W. Ralph Basham served as chief of staff for the new Transportation Security Administration at the Transportation Department. Basham replaces Brian Stafford, who was at the helm of the Secret Service for nearly four years and announced last year that he would retire from the government in January. Stafford's last day is Jan. 24.** Before taking the job at the Transportation Department, Basham was director of the Federal Law Enforcement Training Center. From 1970 to 1998, he worked at the Secret Service, holding a number of positions.
Source: http://www.usatoday.com/news/washington/2003−01−08−secret−service−director_x.htm

14. *January 08, New York Times* — **Report criticizes FEMA's handling of 9/11 economic claims.** An internal review of the Federal Emergency Management Agency's performance after

the Sept. 11 terror attack has concluded that **the agency should have been more flexible and fair in helping people with economic losses. The agency also needs to coordinate better with other government agencies and charities in future disasters, the review concluded.** The report, by FEMA's Office of Inspector General, echoed complaints that have been compounding for months about an agency that has struggled to cope with a disaster without precedent in nature, scale or cost. The 76−page report, which was released yesterday to members of Congress, did praise the agency for doing its best to help as many people as possible within its guidelines. **Still, in fairly blunt language, the inspectors provided a long list of shortcomings and recommendations. And, in an indication of just how charged the subject of the relief effort still remains, the report also included some comments from federal and state officials challenging some of the report's preliminary findings.**
Source: http://www.nytimes.com/2003/01/08/nyregion/08FEMA.html

15. *January 08, Detroit Free Press* — **Passport services catch on.** As national security concerns broaden and local government budgets tighten, cities nationwide are turning to an unusual moneymaker: U.S. passport services. Southfield, Michigan, the latest city to offer the service, will start taking applications today. The new service is expected to put passports into the hands of at least 500 people a year, City Clerk Nancy Banks said. Since Sept. 11, 2001, many more travelers have become concerned about having credible identification and proof of citizenship, Banks said. Passports, which are issued by the U.S. State Department, provide both. **In addition, passport processing could generate $15,000 annually −− $30 per passport −− for the City of Southfield, Banks said. The income could help offset cuts in the city's $120−million budget in lean times, city officials said. There are about 150 sites where people can apply for a passport in Michigan. Since the federal government allowed local government administrators to process passport applications in 1997, more than 300 municipalities have offered the service, State Department spokesman Stuart Patt said.**
Source: http://www.freep.com/news/locoak/npass6_20030106.htm

[Return to top]

Emergency Services Sector

16. *January 08, State of New Jersey* — **New Jersey opens homeland security center.** The state−of−the−art facility will serve as the focal point for Department of Military and Veterans Affairs and the New Jersey Army and Air National Guards' involvement in domestic security activities within New Jersey. **The center will: (1)provide military assistance to civil authorities in response to local, state and federal − emergencies, natural disasters and homeland security issues; (2) provide command and control of NJ Army and Air National Guard soldiers and Airman ordered to State Active Duty; and (3) be able to plan and prepare for homeland security operations to include responding to attacks directed at the population and infrastructure of New Jersey.**
Source: http://www.state.nj.us/cgi−bin/governor/njnewsline/view_article.p l?id=995

[Return to top]

Information and Telecommunications Sector

17. *January 06, Computerworld* — **American Airlines secures wireless LANs in Denver.** Last January it was discovered that the wireless local area networks (LANs) American Airlines Inc. had been operating at their Denver International Airport (DIA) terminal were highly vulnerable to hackers. White Hat Technologies Inc., a Colorado−based security firm, found **they had been operating without any encryption and had even pasted the IP addresses of curbside terminals on the monitors.** A test at DIA on December 20 by White Hat was **unable to detect a single airline wireless network operating without encryption protection**, said Thubten Comerford, CEO of White Hat. In addition, American had not only removed the IP addresses from its OneStop self−service kiosks, but it had also added Cisco Systems Inc.'s Lightweight Extensible Authentication Protocol (LEAP) authentication technology on top of the standard 40−bit Wired Equivalent Privacy (WEP) encryption. LEAP is an authentication algorithm that leverages the 802.1x framework and provides dynamic, per−user WEP keys to protect data in transit. On the downside, Comerford said **the recent test of the DIA facility still managed to pick up a suspected rogue access point (AP), as well as a significant number of vulnerable wireless transmissions emanating from public traveler lounges and frequent−flier clubs throughout the airport.** "The biggest danger at DIA is the sniffing of sensitive information being transmitted by travelers. Few, if any, airports have addressed this security vulnerability, [and] **few airports or airlines warn travelers of the danger of using the wireless networks**," Comerford said.
Source: http://www.idg.net/go.cgi?id=779363

18. *January 06, CERT/CC* — **CERT Vulnerability Note VU#412115: "Network device drivers reuse old frame buffer data to pad packets".** The Ethernet standard (IEEE 802.3) specifies a minimum data field size of 46 bytes. If a higher layer protocol such as IP provides packet data that is smaller than 46 bytes, the device driver must fill the remainder of the data field with a "pad". For IP datagrams, RFC1042 specifies that "the data field should be padded (with octets of zero) to meet the IEEE 802 minimum frame size requirements." Researchers from @stake Inc., a digital security company in Cambridge, Mass, have discovered that, **contrary to the recommendations of RFC1042, many Ethernet device drivers fail to pad frames with null bytes. Instead, these device drivers reuse previously transmitted frame data to pad frames smaller than 46 bytes. This constitutes an information leakage vulnerability that may allow remote attackers to harvest potentially sensitive information.** Depending upon the implementation of an affected device driver, the leaked information may originate from dynamic kernel memory, from static system memory allocated to the device driver, or from a hardware buffer located on the network interface card.
Source: http://www.kb.cert.org/vuls/id/412115

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 www.securityfocus.com

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 1433 (ms−sql−s), 80 (http), 139 (netbios−ssn), 445 (microsoft−ds), 4662 (???), 135 (???), 21 (ftp), 53 (domain), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

19. *January 08, Central Intelligence Agency* — **Unclassified report to Congress on the acquisition of technology relating to weapons of mass destruction and advanced conventional munitions.** On Tuesday, the U.S. Central Intelligence Agency released its unclassified report to Congress on the acquisition of technology relating to weapons of mass destruction and advanced conventional munitions for the period from July 1, 2002 to December 31, 2002. **The report analyzes the acquisition activities (including solicitation, negotiations, contracts, and deliveries) related to weapons of mass destruction (WMD) and advanced conventional weapons of the countries of Iran, Iraq, North Korea, Libya, Syria, Sudan, India, and Pakistan.** Countries that have substantial WMD programs, as well as countries that demonstrated little WMD acquisition activity of concern, were excluded from the report.
Source: http://www.cia.gov/cia/publications/bian/bian_jan_2003.htm

20. *January 08, Associated Press* — **E−mail attributed to bin Laden deputy.** An e−mail purportedly from an al Qaeda chief, posted on a Web site Tuesday, says Americans should be killed and that Sept. 11 helped the cause of Islam. **The 150−word message — allegedly from Ayman al−Zawahri, Osama bin Laden's top deputy — was posted on the Islamic affairs site of a lawyer who spent time in prison with al−Zawahri. In Washington, U.S. intelligence officials said it was plausible the message was from al−Zawahri, but they could not be certain.** Al−Zawahri, an Egyptian, is bin Laden's doctor and spiritual adviser. Both he and bin Laden have recently issued audio statements that convinced American officials they are alive and at large.
Source: http://story.news.yahoo.com/news?tmpl=storyp_on_re_mi_ea/egypt_bin_laden_deputy_1

21. *January 08, Associated Press* — **U.S. has major holes against bio attack.** The United States has some serious holes in its defenses against the kind of biological weapons the military assumes Iraq has, the Army's top biological defense expert said Wednesday. **The Pentagon has**

few or no vaccines or treatments for several biological weapons Iraq has acknowledged producing, such as botulinum toxin, said Col. Erik Henchal, head of the Army's biological defense laboratory. Other holes in the military's biological defenses include the lack of good vaccines or treatments for plague, various viruses which cause the brain inflammation called encephalitis and bacterial poisons called staphlococcal enterotoxins, Henchal said. "We're trying to fill those holes as best we can," said Henchal, who directs the Army's Medical Research Institute of Infectious Diseases, or USAMRIID. For example, the Army lab has developed vaccine−like preventative treatments for the seven forms of deadly botulinum poison but hasn't had the money to get them into full−scale production, he said. **Military officials assume Iraq has biological weapons including the smallpox virus, and Iraq can produce novel germ weapons such as antibiotic−resistant bacteria, Henchal said.** He said the Army is sending its only mobile biological testing unit to the Persian Gulf this week. The Maryland−based unit does rapid testing to help confirm an attack with germ weapons.
Source: http://www.usatoday.com/news/washington/2003−01−08−bio−attack_x.h tm

22. *January 08, Reuters* — **New arrest as UK terror police hunt deadly poison.** British anti−terrorist police hunting for a potential cache of deadly ricin said Wednesday they had arrested another man after traces of the poison were found in a north London apartment. Anti−terrorist police are now questioning seven men after seizing the poison, which some experts have linked to al Qaeda, in raids Sunday. "The arrest is part of ongoing inquiries by the anti−terrorist branch and is linked to Sunday's arrests," a London police spokesman said, adding that no further information would be released. One security source told Reuters the first six men were Algerians whose likely intention was to infect people using a poisoned cream. **Police fear the traces of ricin and equipment they found in a Victorian terraced flat above an innocuous pharmacy could be just the tip of the iceberg. Security sources said large amounts of the poison could still be in the hands of extremists in Britain or abroad.** As police only found a small amount of the poison, officers were on an urgent hunt for any other secret stockpiles that might be used to sow terror.
Source: http://www.washingtonpost.com/wp−dyn/articles/A27622−2003Jan8.htm l

[Return to top]

NIPC Information Bulletins − Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

NIPC CyberNotes − CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure−related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:	Melissa Conaty (202−324−0354 or mconaty@fbi.gov) Kerry J. Butterfield (202−324−1131 or kbutterf@mitre.org)
Distribution Information	NIPC Watch and Warning Unit (202−323−3204 or nipc.watch@fbi.gov)

NIPC Disclaimer